|  |
| --- |
| 大邑县第二人民医院 关于“终端安全管理系统”采购项目 |
| 询 |
| 价 |
| 通 |
| 知 |
| 书 |
| 中国·四川·成都 |
| 大邑县第二人民医院  关于“终端安全管理系统”采购项目 |
| 询价通知书 |
| 大邑县第二人民医院（采购人）拟对关于“终端安全管理系统”采购项目以询价方式进行采购，欢迎广大响应人参加该项目的采购。 |
| 一、项目编号：20250701 |
| 二、项目名称：终端安全管理系统 |
| 三、预算金额（最高限价）：4.95万元。 |
| 1. 采购内容：大邑县第二人民医院拟采用询价比选采购该项目，内容即为采购项（终端安全管理系统）。   终端安全管理系统：预算控制价为4.95万元，需求及参数如附件1。 |
| 五、响应人参加询价应当具备的资格条件： |
| 1、符合《中华人民共和国政府采购法》第二十二条的相关规定； |
| 2、响应人参加本次采购活动前三年内，在经营活动中没有重大违法违规记录（提供信用报告及响应人无违法违规行为的承诺书，在采购结果公示期结束前一经查实有违法违规将取消其响应人资格或中标候选人资格）。 |
| 六、响应人参加询价应当提供的资格证明材料（均需加盖单位公章）： |
| 1、企业信用报告； |
| 2、法定代表人或单位负责人身份证复印件； |
| 3、法定代表人或单位负责人授权委托书原件及授权代表的身份证复印件； |
| 4、①比选申请人若为企业法人：提供“统一社会信用代码营业执照”；未换证的提供“营业执照、税务登记证、组织机构代码证或三证合一的营业执照”；②若为事业法人：提供“统一社会信用代码法人登记证书”；未换证的提交“事业法人登记证书、组织机构代码证”；③若为其他组织：提供“对应主管部门颁发的准许执业证明文件或营业执照”；④若为个体工商户：提供“统一社会信用代码营业执照副本”或“营业执照、税务登记证”⑤若为自然人：提供“身份证明材料”。以上均提供复印件。  上述证明材料均须加盖公章（鲜章），相关证明材料附后。 |
| 七、报名时间及地点： |
| 报名时间：2025年7月1日至 2025年 7月7日，上午 08：30-下午 17：00（北京时间）。 |
| 报名地点：成都市大邑县第二人民医院后勤科。 |
| 八、递交响应文件截止时间：2025年7月7日下午17:00（北京时间）。 |
| 九、递交响应文件地点：响应文件必须在递交响应文件截止时间前送达大邑县第二人民医院后勤科。逾期送达、未密封和标注错误的响应文件，恕不接收。本次采购不接收邮寄的响应文件。 |
| 十、评审时间：采购人根据实际情况确定评审时间。 |
| 十一、联系人及联系电话： |
| 采 购 人：四川省成都市大邑县第二人民医院 |
| 联 系 人：钱老师 |
| 联系电话：028-69335120 |
| 地 址：大邑县安仁镇千禧街181号附2号 |
|  |
|  |
| 大邑县第二人民医院 |
|  |
| 关于“终端安全管理系统”项目 |
|  |
| 报价函 |
| |  |  |  |  | | --- | --- | --- | --- | | 项目编号 | 项目名称 | 报价（万元） | 备注 | |  |  |  |  | |  |  |  |  | |  |  |  |  | |
| 根据实际情况调整报价函 |
| 报价单位： |
| 联 系 人： |
| 电 话： |
| 报价日期： |

附件1：

终端安全管理系统

需求：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **产品名称** | **单位** | **数量** | **备注** |
|  | 终端安全管理系统 | 套 | 1 | 详细技术指标见下列参数表 |

参数：

1. ★含控制中心一套，配置要≥180点PC端功能授权，功能授权包括：提供杀毒+勒索防护+漏洞管理+资产管理+安全体检+终端管控+漏洞免疫模块，客户端系统默认支持WindowsXP/VISTA/WIN7/WIN8/WIN10。；配置≥5点Windows 服务器端功能授权，功能授权包括：杀毒+勒索防护+漏洞管理+资产管理模块，客户端系统默认支持Windows-server；三年软件及病毒库升级。
2. ▲管控中心后台数据库需使用国产数据库，且具备自主知识产权，符合国家对软件自主可控的要求，需提供数据库的《信息技术产品自主原创性测评证书》。**（提供国产数据库，国家网络与信息系统安全产品质量监督检验中心颁发的测评证书复印件并加盖供应商公章）**
3. ▲管控中心后台国产数据库支持AES、DES及国密SM算法。**（提供国产数据库支持AES、DES等国密算法，CNAS或CMA的测试报告复印件，并加盖供应商公章）**
4. ▲提供多引擎查杀矩阵，至少包括云查杀引擎、大数据特征引擎、自学习智能引擎以及脚本引擎等4个引擎，提供全面的反病毒能力，客户端支持以图形化方式展示各个引擎的信息；**（提供对应功能截图，并加盖供应商公章）**
5. ▲针对Windows64位操作系统，可利用CPU的硬件虚拟化机制，增强64位系统的安全防护，提供核晶防护功能。**（提供对应功能截图，并加盖供应商公章）**
6. 支持对管理员账户登录或高危操作进行多因子认证，包括动态口令二次认证且可通过微信小程序查看动态口令，支持多因子认证的高危操作包括文件分发、账号添加修改、重置密码、消息推送等；
7. 具备云端样本鉴定能力，云端具备310亿+样本数据，有效针对各种病毒文件进行查杀；
8. ▲产品支持对日常办公文档进行备份还原能力，支持对.doc、docx、xls、xlsx、ppt、pptx、pdf等文档进行自动备份，可以自定义备份格式。必要时，可将文件进行还原。备份途径支持本地加密备份和办公云盘备份，备份方式包括修改前备份以及修改后定时备份，备份范围支持全盘备份和指定路径备份。支持对常见100余种勒索病毒加密的文档进行解密；**（提供对应功能截图，并加盖供应商公章）**
9. 提供APT全景雷达：内置55个APT组织情报信息（包括介绍、MD5、CC域名、常用漏洞等）、25000+APT IOC情报库，支持按照已知的APT情报对内网进行APT攻击痕迹检测，判断终端是否存在已知APT攻击行为；支持对存在APT漏洞风险的终端进行分类统计；
10. 提供针对域名、IP、URL、文件hash、邮箱地址等信息进行威胁查询，可获取解析记录、相关证书、子域名信息、WHOIS日志、通讯样本、资产状态、恶意网址、公开报告等信息；
11. 支持漏洞相关安全组件配套使用，增强终端漏洞检测能力，，包含：驱动大师、主页修复、Win7 盾甲 。强化产屁功能，丰富扫描内容；
12. 服务端可设置补丁生效策略，补丁安装完成后可按照提醒一次、间隔提醒（分钟）、规定时间段重启的方式，提醒客户端用户重启系统，以使补丁及时生效；
13. 对管控中心所守护的终端量和防护成果进行统计。统计项分别为守护终端数量、累计查杀病毒、累计漏洞修复。全网终端最新发生的安全事件进行发现，以时间轴方式滚动播报，方便用户及时了解最新的安全事件动态，及时进行干预、处置操作，另有终端类型分布、组织架构展示、病毒类型TOP5、病毒检出趋势、未修复漏涧类型分布、漏涧检出趋势等内容；
14. 支持对客户端下发多种扫描指令，包括快速扫描、全盘扫描、强力扫描等；快速扫描支持快速对客户端系统设置、常用软件、内存活跃程序、开机启动项以及系统关键位置进行扫描；全盘扫描支持对客户端全部路径进行文件扫描；强力扫描能够在执行快速扫描、全盘扫描或自定义扫描时，强制扫描客户端所有文件包含白名单。支持设置扫描任务有效期，过了有效期后，未完成扫描的终端尝试结束扫描任务，未开始扫描的终端不再执行此任务；
15. 支持对客户端设置防感染模式，扫描到感染型病毒时，自动进入防感染模式，重新开始全盘扫描并阻止恶意样本反复感染文件；
16. 支持非法外联管理，支持终端探测、互联网探测两种探测方式。其中终端探测支持解析域名、TCP、Ping三种探测方式，互联网出口探测支持探测客户端互联网出口地址，通过返回值来判断终端是否已经发生外联行为，并可设置出口白名单，对白名单内的出口不进行违规外联限制；
17. 支持开启蓝屏修复功能，当安装补丁出现蓝屏时可恢复系统；
18. ▲支持进程红名单，红名单提供必须启动和进程保护两种控制模式。必须启动模式要求客户端必须运行名单中的进程，为了强化进程安全性，MD5验证失败的进程可排除在启动范围内；进程保护模式支持对名单中的进程提供保护，避免被第三方恶意结束；**（提供对应功能截图，并加盖供应商公章）**
19. SSID信息统计：可统计终端连接过的无线SSID信息，在控制中心形成SSID库，可统计SSID的名称、首次发现时间、mac地址、是否可联通互联网，来源等信息；
20. 支持Windows终端敏感信息扫描功能，提供敏感信息库，通过通配符和正则表达式的方式自定义敏感信息扫描规则，支持多规则组合成模板，扫描终端存在的敏感文件信息。支持Office、PDF、WPS等，支持多层嵌窖，能够识别加密文件，支持全部和增量扫描，支持全盘扫描、指定路径扫描，可指定扫描文件的后缀。支持根据终端资源情况变化《CPU、内存、I0等)、文件大小优化扫描过程。
21. ▲为保障终端安全管理系统控制中心的安全稳定运行，终端安全管理系统控制中心后台操作系统需经过满足《信息安全技术主机安全加固系统安全技术要求 GA/T1393-2017》增强级标准专业安全加固工具进行加固。**（提供安全加固工具具有CNAS或CMA的测试报告复印件，并加盖供应商公章）**
22. ▲安全加固工具支持对操作系统安全基线进行检测、加固、恢复**（提供对应功能截图，并加盖供应商公章）**
23. ▲安全加固工具支持应用程序白名单，只有属于白名单列表的可执行程序可以运行，不在列表中的所有可执行程序都不能执行。**（提供对应功能截图，并加盖供应商公章）**
24. ▲安全加固工具支持文件的强访问控制权限：可以细化和严格定义用户对文件的访问权限（剥离超级用户权限），也可以结合强访问控制模型定义用户对文件的访问权限。**（提供对应功能截图，并加盖供应商公章）**
25. ▲安全加固工具支持微隔离策略配置，微隔离支持标签和标签、标签和主机、主机和主机之间的隔离策略配置。**（提供对应功能截图，并加盖供应商公章）**

▲安全加固工具需支持展示所有主机的主机信息、主机分组、agent状态、风险状态、告警数量、安全评分及性能信息。**（提供对应功能截图，并加盖供应商公章）**

注：★表示实质性条款。▲表示相对重要的技术参数。